MIGLIACCIO & RATHOD LLP
Matthew A. Smith (CA No. 309392)
201 Spear St., Ste 1100
San Francisco, CA 94105
Tel: (415) 489- 7004
msmith@classlawdc.com

Nicholas Migliaccio (*pro hac vice* anticipated)
Jason Rathod (*pro hac vice* anticipated)
Bryan G. Faubus (*pro hac vice* anticipated)
412 H St. NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730
nmigliaccio@classlawdc.com
jrathod@classlawdc.com
bfaubus@classlawdc.com

Attorneys for Plaintiffs and Proposed Class

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA

MATTHEW MARDEN and MICHELLE IGOE, individually and on behalf of all others similarly situated, Plaintiff, v. LMND MEDICAL GROUP, INC., d/b/a LEMONAID HEALTH, a California Professional Corporation, LMND MEDICAL GROUP, a Kansas Professional Association, LMND MEDICAL GROUP, a New Jersey Professional Corporation, and LMND MEDICAL GROUP, a Texas Professional Association, Defendants.	**Case No.** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Matthew Marden and Michelle Igoe ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through undersigned counsel, hereby allege the following against Defendants LMND Medical Group, Inc., d/b/a Lemonaid Health, a California Professional Corporation, LMND Medical Group, a Kansas Professional Association, LMND Medical Group, a New Jersey Professional Corporation, and LMND Medical Group, a Texas Professional Association

(collectively, "Lemonaid" or "Defendants"). Facts pertaining to Plaintiffs and their personal experiences and circumstances are alleged based upon personal knowledge, and all other facts herein are alleged based upon the investigation of counsel and upon information and good faith belief.

NATURE OF THE ACTION

1. This is a class action lawsuit for damages and injunctive relief arising from Defendants' unlawful practice of disclosing Plaintiffs' and Class members' individually identifiable health information ("IIHII") and protected health information ("PHI") (referred to herein collectively as "Private Information") to unauthorized third parties including, but not limited to, Meta Platforms, Inc. d/b/a Meta (also referred to herein as "Facebook"), Google LLC, and TikTok Inc. (collectively, the "Pixel Information Recipients").

2. Defendants own, control, and maintain the website https://www.lemonaidhealth.com/ (referred to herein as the "Website" or "Defendants' Website"), a website which requires individuals to share highly sensitive IIHI and PHI in order to create accounts and to participate in highly sensitive and personal health screenings and receive treatment plans.

3. Defendants installed and implemented "pixels" and similar tracking technologies such as those made available by the Pixel Information Recipients (referred to herein as the "Pixels") on the Website.

4. Invisible to the naked eye, each of the Pixels collect and transmit information from the user's browser to the corresponding Pixel Information Recipient as the user enters information into the Website. The Pixels secretly enable the unauthorized transmission and disclosure of Plaintiffs' and Class Members' IIHI and PHI by Defendants.

5. Defendants also installed and implemented the Facebook Conversions Application Programming Interface ("Conversions API") on the Website. Conversions API serves the same purpose as the Pixels in that it surreptitiously collects and transmits Private Information to Facebook. Unlike the Pixels, however, Conversions API functions from Defendants' servers and therefore cannot be stymied by use of anti-Pixel software or other workarounds. Defendants secretly enabled

additional unauthorized transmissions and disclosures of Plaintiffs' and Class members' IIHI and PHI to Facebook by implementing the Conversions API.[1]

6. Through the use of the Pixels and Conversions API, Defendants' Website directs Plaintiffs' and Class members' communications to automatically be sent to the servers of the corresponding Pixel Information Recipients. This occurs on every webpage in which Defendants installed the Pixels and for which Defendants enabled Conversions API.[2]

7. Thus, operating as implemented by Defendants, the Pixels and Conversions API allow the Private Information that Plaintiffs and Class members submit to them in confidence to be unlawfully disclosed to the Pixel Information Recipients alongside the individual's unique personal identifiers, including his or her Facebook ID and other identifying information pertaining to any accounts they may have with any of the Pixel Information Recipients.

The Tracking Pixel

8. A "pixel" is a piece of code that "tracks the people and the types of actions they take"[3] as they interact with a website, including how long a person spends on a particular webpage, which buttons the person clicks, which pages they view, the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), and more.

9. Pixels are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting—*i.e.*, serving online advertisements to people who have previously engaged with a business's website—and other marketing.

10. Here, a user's web browser executes the Pixels via instructions within each webpage of Defendants' Website to communicate certain information (within parameters set by Defendants) directly to the corresponding Pixel Information Recipients.

---

[1] "Conversions API works with your Facebook Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited June 29, 2023).

[2] "Server events are linked to a dataset ID and are processed like events sent via the [Facebook] Pixel … This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." *See* https://developers.facebook.com/docs/marketing-api/conversions-api (last visited June 29, 2023).

[3] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited June 29, 2023).

11. The Pixels can also share the user's identifying information for easy tracking via the "cookies"[4] stored on their computer by any of the Pixel Information Recipients with which they have an account. For example, Facebook stores or updates a Facebook-specific cookie every time a person accesses their Facebook account from the same web browser. The Facebook Pixel can access this cookie and send certain identifying information like the user's Facebook ID to Facebook along with the other data relating to the user's Website inputs. The same is true for the other Pixel Information Recipients, which also create cookies that are stored in the user's computer and accessed by the Pixels to identify the user.

12. The Pixels are programmable, meaning that Defendants control which of the webpages on the Website contain the Pixels, and which events are tracked and transmitted to the Pixel Information Recipients.

13. Defendants have utilized the Pixels and other tracking technologies since at least January 2017.

14. Defendants used the data they collected from Plaintiffs and Class members, without their consent, in an effort to improve their advertising and bolster their revenues.

Conversions API

15. The Facebook Conversions API and similar tracking technologies allow businesses to send web events, such as clicks, form submissions, keystroke events, and other user actions performed by the user on the Website, from their own servers to Facebook and other third parties.[5]

16. The Conversions API creates a direct and reliable connection between marketing data (such as website events and offline conversations) from Defendants' server to Facebook.[6] In doing so, Defendants store Plaintiffs' and Class members' Private Information on their own server and then transmit it to unauthorized third parties.

---

[4] "Cookies are small files of information that a web server generates and sends to a web browser Cookies help inform websites about the user, enabling the websites to personalize the user experience." *See* https://www.cloudflare.com/learning/privacy/what-are- cookies/ (last visited June 29, 2023).

[5] https://revealbot.com/blog/facebook-conversions-api/ (last visited June 15, 2023).

[6] *See* https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited June 29, 2023).

17. The Conversions API is an alternative method of tracking versus the Facebook Pixel because no privacy protections on the user's end can defeat it. This is because it is "server-side" implementation of tracking technology, whereas the Pixels are "client-side," *i.e.*, executed on users' computers in their web browsers.

18. Because Conversions API is server-side, it cannot access the Facebook Cookie to retrieve the Facebook ID.[7] Therefore, other roundabout methods of linking the user to their Facebook account are employed.[8]

19. Facebook has an entire page within its developers' website about how to de-duplicate data received when both the Facebook Pixel and Conversions API are executed.[9]

20. Conversions API tracks the user's website interaction, including Private Information being shared, and then transmits this data to Facebook and other third parties. Facebook markets Conversions API as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."

This Lawsuit

21. Plaintiffs bring this lawsuit on behalf of similarly situated individuals whose sensitive Private Information was intentionally, recklessly, and/or negligently disclosed to the Pixel Information Recipients through Defendants' unauthorized utilization of the Pixels, Conversions API, and other similar tracking technologies.

---

[7] "Our systems are designed to not accept customer information that is unhashed Contact Information, unless noted below. Contact Information is information that personally identifies individuals, such as names, email addresses, and phone numbers, that we use for matching purposes only." *See* https://developers.facebook.com/docs/marketing- api/conversions-api/parameters/customer-information-parameters/ (last visited June 29, 2023).

[8] "Sending additional customer information parameters may help increase Event Match Quality. Only matched events can be used for ads attribution and ad delivery optimization, and the higher the matching quality, the better." https://developers.facebook.com/docs/marketing-api/conversions-api/best-practices/#req- rec-params (last visited June 29, 2023).

[9] *See* https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel-and-server-events (last visited June 29, 2023).

22. The Private Information that the Pixels and Conversions API gathered from Defendants' Website and sent to the Pixel Information Recipients included the Private Information that Plaintiffs and Class members submitted to Defendants' Website, including for example, particular health conditions, types of health treatment sought and/or received, age, and other confidential IIHI and PHI.

23. The Pixel Information Recipients in turn use Plaintiffs' and Class members' Private Information for business purposes, including using such information to improve advertisers' ability to target specific demographics and selling such information to third-party marketers who target Plaintiffs and Class members online (*i.e.*, through their Facebook, Instagram, TikTok, and other social media and personal accounts).

24. Here, Plaintiffs and Class members submitted Private Information to Defendants' Website in order to participate in health assessments and other health-related services offered through the Website.

25. Concurrently, this information was communicated from the Website (via the Pixels and Conversions API) to the Pixel Information Recipients: from the Facebook Pixel and Conversions API to Facebook, and from the other Pixels to their respective recipients.

26. In sum, Plaintiffs and Class members provided their Private Information to Defendants by creating accounts, completing health assessments, researching doctors and other health-related services providers, making appointments, reviewing conditions and available treatments, researching prescriptions, and/or purchasing subscription plans and, at all times throughout this process, had a reasonable expectation of privacy in the Private Information Defendants were collecting, including that Defendants would ensure that such Private Information remain secure and protected and only utilized for limited medical and health purposes.

27. Defendants further made express and implied promises to protect Plaintiffs' and Class members' Private Information and maintain the privacy and confidentiality thereof.

28. Prior to a revision implemented on January 17, 2023, Defendants' Notice of Privacy Practices expressly stated "Rest Assured, Lemonaid does not sell, rent, license, or trade your Personal Information."[10]

29. Defendants owed common law, contractual, statutory, and regulatory duties to keep Plaintiffs' and Class members' Private Information safe, secure, and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' Private Information, Defendants assumed legal and equitable duties to patients to protect and safeguard their Private Information from unauthorized disclosure.

30. Defendants, however, failed in their obligations and promises by utilizing the Pixels and Conversions API on the Website as described herein, knowing that such technology would transmit and share Plaintiffs' and Class members' Private Information with the Pixel Information Recipients.

31. While Defendants willfully and intentionally incorporated the Pixels and Conversions API into the Website, Defendants never disclosed to Plaintiffs or Class members that they shared their sensitive and confidential assessment responses via the Website with third parties. As a result, Plaintiffs and Class members were unaware that their IIHI and PHI were being surreptitiously transmitted to the Pixel Information Recipients as they participated in health assessments on Defendants' Website.

32. Despite the stigmas that unfortunately are so often associated with certain health issues and treatments, Defendants intentionally chose to put their profits over the privacy of their users, which number several million. The unilateral disclosure of users' Private Information in this manner is unquestionably a violation of HIPAA, among other statutory and common laws.

33. The disclosure of Plaintiffs' and Class Members' Private Information via the Pixels contravenes the letter and spirit of HIPAA's "Standards for Privacy of Individually Identifiable

[10] Lemonaid Privacy Policy (Apr. 18, 2022), *available at* https://web.archive.org/web/20220422115411/https://www.lemonaidhealth.com/legals/privacy-policy (last visited June 16, 2023).

Health Information" (also known as the "Privacy Rule") which governs how health care providers must safeguard and protect Private Information. [11]

34. The HIPAA Privacy Rule sets forth policies to protect all IIHI that is held or transmitted by a covered entity such as Cerebral. These are the 18 HIPAA Identifiers that are considered personally identifiable information because this information can be used to identify, contact, or locate a specific person or can be used with other sources (such as a person's Facebook account) to identify a single individual. When IIHI is used in conjunction with one's physical or mental health or condition, health care, and/or one's payment for that health care, it becomes PHI.[12]

35. While healthcare entities regulated under HIPAA may use third-party tracking tools, such as Google Analytics or the Facebook Pixel, they can do so only in a very limited way, to perform analysis on data key to operations.

36. Simply put, further to the HIPAA Privacy Rule, covered entities such as Defendant are simply ***not*** permitted to use tracking technology tools (like pixels) in a way that exposes patients' Private Information to any third party without express and informed consent.

37. Lest there be any doubt of the illegal nature of Defendant's practice, the Office for Civil Rights ("OCR") at HHS has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (the "HHS OCR Bulletin"), that the unlawful transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or

---

[11] HHS.gov, The HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited June 29, 2023).

[12] *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, HHS.GOV (last visited March 21, 2023) (HIPAA Identifiers include name; address (all geographic subdivisions smaller than state, including street address, city county, and zip code); all elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age); telephone numbers; email address; medical record number; health plan beneficiary number; account number; device identifiers and serial numbers; web URL; internet protocol (IP) address; and any other characteristic that could uniquely identify the individual).

> any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[13]

38. Defendants breached their obligations to Plaintiffs and the Class members in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure the Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share patients' Private Information; (iii) failing to obtain the consent of patients, including Plaintiffs and Class members, to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiffs' and Class members' Private Information through the Pixels and Conversions API; (v) failing to warn Plaintiffs and Class members of such sharing and disclosures; (vi) otherwise failing to design and monitor the Website to maintain the confidentiality and integrity of patients' Private Information.

39. Plaintiffs and Class members have suffered injury as a result of Defendants' conduct. These injuries include (i) invasion of privacy, (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the transmissions of their Private Information to the Pixel Information Recipients, (iii) loss of the benefit of the bargain, (iv) diminution of value of the disclosed Private Information, (v) statutory damages, and (vi) the continued and ongoing risk to their Private Information. Plaintiffs seek to remedy these harms and bring causes of action for: (1) negligence; (2) invasion of privacy, (3) breach of confidence; (4) unjust enrichment; (5) violations of the Electronics Communication Privacy Act ("ECPA"), 18 U.S.C. § 2511(1); (6) violations of the ECPA, 18 U.S.C. § 2511(3)(a); (7) violations of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631; (8) violations of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*; (9) violations of the California Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.*; (10)

[13] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html, HHS.GOV (emphasis added) (last visited June 4, 2023).

violations of the Massachusetts Data Breach Statute, Mass. Gen. Laws § 93H; and (11) violations of the Massachusetts Consumer Protection Act, Mass. Gen. Laws § 93A *et seq.*

PARTIES

A. Plaintiff Matthew Marden

40. Plaintiff Matthew Marden is a citizen of the state of Massachusetts residing in Marlborough and brings this action in an individual capacity and on behalf of all others similarly situated.

41. On multiple occasions beginning in or around 2019, Plaintiff Marden utilized Defendants' Website on his personal electronic devices to create an account, research conditions and treatments, search for doctors, and schedule appointments. In the process of using Defendants' services, Plaintiff Marden was required to disclose highly sensitive IIHI and PHI to Defendants.

42. While Plaintiff Marden was a user of Defendants' services, he never consented to or authorized the use of his Private Information by third parties or to Defendants enabling third parties to access, interpret, and use such Private Information.

43. Plaintiff Marden had a Facebook account while he used Defendants' services and he accessed Defendant's Website while logged into his Facebook account on the same device. After providing his Private Information to Defendants through the Website, Plaintiff Marden immediately began seeing targeted health ads as he scrolled through his accounts.

B. Plaintiff Michelle Igoe

44. Plaintiff Michelle Igoe is a citizen of the state of Massachusetts residing in Norwood and brings this action in an individual capacity and on behalf of all others similarly situated.

45. On multiple occasions beginning in the spring of 2020, Plaintiff Igoe utilized Defendants' Website on her personal electronic devices to create an account, research conditions and treatments, search for doctors, and make appointments. In the process of using Defendants' services, Plaintiff Igoe was required to disclose highly sensitive IIHI and PHI to Defendants.

46. While Plaintiff Igoe was a user of Defendants' services, she never consented to or authorized the use of her Private Information by third parties or to Defendants enabling third parties to access, interpret, or use such Private Information.

47. Plaintiff Igoe had a Facebook account while she used Defendants' services and she accessed Defendant's Website while logged into her Facebook account on the same device. After providing her Private Information to Defendants through the Website, Plaintiff Igoe immediately began seeing targeted health ads as she scrolled through her account.

48. Pursuant to the systematic process described in this Complaint, the Private Information that Plaintiffs entrusted to Defendants was disclosed to the Pixel Information Recipients without Plaintiffs' knowledge or consent.

49. Defendants transmitted and/or enabled the transmission of such Private Information without Plaintiffs' knowledge, consent, or express written authorization. By failing to receive such requisite consent, Defendants breached confidentiality and unlawfully disclosed each Plaintiff's Private Information.

50. But for Plaintiffs' status as users of Defendants' services and Defendants' express and implied promises regarding the security of their Private Information, Plaintiffs would not have disclosed such information to Defendants.

C. Defendants

51. Defendant LMND Medical Group, Inc., is a Professional Corporation incorporated in California and headquartered in San Francisco.

52. Defendant LMND Medical Group, is a Professional Association formed in Kansas ("Lemonaid Kansas").

53. Defendant LMND Medical Group, a Professional Corporation, was incorporated in New Jersey ("Lemonaid New Jersey").

54. Defendant LMND Medical Group, a Professional Association, was formed in Texas ("Lemonaid Texas, and together with Lemonaid Kansas and Lemonaid New Jersey, the "Lemonaid State Entities").

55. The Lemonaid State Entities are affiliates of LMND Medical Group, Inc., and assist LMND Medical Group, Inc. in the provision of health services to Class members in Kansas, Texas, and New Jersey.

56. Collectively, Defendants focus on the provision of health care and related services. On the Website, Defendants tout their mission "to break down barriers that limit people from getting quality healthcare, empowering them to live happier lives.[14] Defendants offer counseling and treatment for a variety of health issues, including some issues relating to mental health (*e.g.*, anxiety and depression), sexual health (*e.g.*, erectile dysfunction and treatment and testing for sexually transmitted infections), reproductive health (*e.g.*, emergency contraception), and a variety of other health conditions.[15]

JURISDICTION & VENUE

57. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because Plaintiffs and many putative class members are citizens of a different state than Defendants. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

58. This Court has personal jurisdiction over Defendants because they operate and maintain their principal place of business in this District. Further, Defendants are authorized to and regularly conduct business in this District and make decisions regarding corporate governance and management of the Website in this District, including decisions regarding the privacy of patients' IIHI and PHI and the incorporation of the Pixels, Conversions API, and other tracking technologies.

59. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because: a substantial part of the events giving rise to this action occurred in this District, including decisions made by Defendants' governance and management personnel or inaction by those individuals that led to the unauthorized sharing of Plaintiffs' and Class members' Private Information; Defendants' principal place of business is located in this District; Defendants collect and redistribute Class members' Private Information in this District; and Defendants caused harm to Class members residing in this District. Additionally, Defendants' Terms of Use sets forth a requirement that any litigation

---

[14] Our Mission, https://www.lemonaidhealth.com/our-story (last visited June 16, 2023).
[15] *See* https://www.lemonaidhealth.com/ (last visited June 16, 2023).

against Defendants shall be filed in state or federal courts in Santa Clara County, California.[16]

FACTUAL ALLEGATIONS

60. Defendants have utilized the Pixels and other tracking technologies since at least January 2017. Defendants installed the Pixels and Conversion API, as well as other tracking technologies, on many (if not all) of the webpages within the Website and programmed or permitted those webpages to surreptitiously share patients' private and protected communications with the Pixel Information Recipients—communications that included Plaintiffs' and Class members' Private Information.

61. In order to understand Defendants' unlawful data-sharing practices, it is important to first understand some of the basic web design and tracking tools at issue.

A. Defendants' Method of Transmitting Plaintiffs' and Class Members' Private Information via Pixel and Conversions API

62. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as a computer, tablet, or smartphone) accesses web content through a web browser (*e.g.*, Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

63. Every website is hosted by a computer "server" that holds the website's contents. The entity(ies) in charge of the website exchange communications with users' client devices as their web browsers query the server through the internet.

64. Web communications consist of Hypertext Transfer Protocol ("HTTP") or Hypertext Transfer Protocol Secure ("HTTPS") requests and HTTP or HTTPS responses, and any given browsing session may consist of thousands of individual HTTP requests and HTTP responses, along with corresponding cookies:

a. **HTTP request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP

[16] *See* Terms of Use, www.lemonaidhealth.com/legals/terms-of-use (last visited on June 16, 2023).

Requests. In addition to specifying a particular URL (*i.e.*, web address), GET Requests can also send data to the host server embedded inside the URL and can include cookies. POST Requests can send a large amount of data outside of the URL. (For instance, uploading a PDF for filing a motion to a court.)

b. **Cookies**: a small text file that can be used to store information on the client device that can later be communicated to a server or servers. Cookies are sent with HTTP requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.

c. **HTTP response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP request. HTTP responses may consist of a web page, another kind of file, text information, or error codes, among other data.

65. A patient's HTTP request essentially asks the Defendants' Website to retrieve certain information (such as a set of health screening questions). The HTTP response sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the participant's screen as they navigate Defendants' Website.

66. Every website is comprised of Markup and "Source Code." Source Code is a simple set of instructions that commands the website user's browser to take certain actions when the webpage first loads or when a specified event triggers the code.

67. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP requests quietly executed in the background without notifying the web browser's user.

68. The Pixels are Source Code that does just that—they surreptitiously transmit a Website user's communications and inputs to the corresponding Pixel Information Recipient much like a traditional wiretap. When individuals visit Defendants' Website via an HTTP request to Defendants' server, Defendants' server sends an HTTP response (including the Markup) that displays the webpage visible to the user, along with Source Code (including the Pixels).

69. Thus, Defendants are, in essence, handing its patients a tapped phone and, once the webpage is loaded into the patient's browser, the software-based wiretaps are quietly waiting for private communications on the webpage to trigger the Pixels, which then intercept those communications intended only for Defendants and transmits those communications to the corresponding Pixel Information Recipient.

70. Third parties like the Pixel Information Recipients place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can uniquely identify the user associated with the information intercepted (in this case, highly sensitive Private Information).

71. Defendant intentionally configured Pixels installed on its Website to capture both the "characteristics" of individual patients' communications with the Defendant's Websites (*i.e.*, their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (*i.e.*, the buttons, links, pages, and tabs they click and view).

72. Defendant also deposits cookies named _fbp, _ga_, and _gid onto Plaintiffs' and Class Members' computing devices. These are cookies associated with the third-parties Facebook and Google but which Defendant deposits on Plaintiffs and Class Members' computing devices by disguising them as first-party cookies. And without any action or authorization, Defendant commands Plaintiffs' and Class Members' computing devices to contemporaneously re-direct the Plaintiffs' and Class Members' identifiers and the content of their communications to Facebook and Google.

73. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Defendant's use of the Facebook Pixel. The fbp cookie emanates from Defendant's Website as a putative first-party cookie, but is transmitted to Facebook through cookie synching technology that hacks around the same-origin policy. The __ga and _gid cookies operate similarly as to Google.

74. Furthermore, if the patient is also a Facebook user, the information Facebook receives is linked to the patient's Facebook profile (via their Facebook ID or "c_user id"), which includes other identifying information.

B. Facebook's Platform & its Business Tools.

75. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[17]

76. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendants, to utilize its "Business Tools" to gather, identify, target and market products and services to individuals.

77. Facebook's Business Tools, including the Facebook Pixel, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

78. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[18]

79. Advertisers, such as Defendants, can track other user actions and can create their own tracking parameters by building a "custom event."[19]

80. One such Business Tool is the Facebook Pixel, which "tracks the people and type of actions they take."[20]

---

[17] META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx, INVESTOR.FB.COM (last visited June 29, 2023).

[18] *Specifications for Facebook Pixel Standard Events*, https://www.facebook.com/business/help/402791146561655?id=1205376682832142, FACEBOOK.COM (last visited June 29, 2023); *see*, META PIXEL, GUIDES, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/, FACEBOOK.COM (last visited June 29, 2023); *see also* BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142, FACEBOOK.COM (last visited June 29, 2023); META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/, FACEBOOK. COM (last visited June 29, 2023).

[19] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142, FACEBOOK.COM (last visited June 29, 2023); *see also* META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[20] RETARGETING, https://www.facebook.com/business/goals/retargeting, FACEBOOK.COM (last visited June 29, 2023).

81. When a user accesses a webpage that is hosting the Facebook Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers—traveling from the user's browser to Facebook's server.

82. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's Website—Defendant's own code and Facebook's embedded code.

83. Accordingly, during the same transmissions, the Website routinely provides Facebook with its patients' Facebook IDs, IP addresses, and/or device IDs and the other information they input into Defendant's Website, including not only their medical searches, treatment requests, and the webpages they view, but also their unique personal identifiers including email address and/or phone number. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[21] Plaintiffs' and Class Members identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

84. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. When the website visitor is also a Facebook user, the information collected via the Facebook Pixel is associated with the user's Facebook ID that identifies their name and Facebook profile, *i.e.*, their real-world identity. Likewise, Facebook maintains "shadow profiles" on users without Facebook accounts and links the information collected via the Facebook Pixel to the user's real-world identity using their shadow profile.[22]

---

[21] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited June 29, 2023).

[22] *See* Russell Brandom, *Shadow Profiles Are The Biggest Flaw In Facebook's Privacy Defense*, TheVerge.com (Apr 11, 2018), *available at* https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (*last visited* June 28, 2023).

85. A user's Facebook ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

86. The Private Information disclosed via the Pixel allows Facebook to know that a specific patient is seeking confidential medical care and the type of medical care being sought. Facebook then uses that information to sell advertising to Defendants and other advertisers and/or sells that information to marketers who will online target Plaintiffs and Class members.

87. With substantial work and technical know-how, internet users can sometimes circumvent the browser-based wiretap technology of the Pixels. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that even savvy users cannot evade. Facebook's workaround is called Conversions API. Conversions API is effective because it transmits directly from the host server and does not rely on the user's web browser.

88. Thus, the communications between patients and Defendants, which are necessary to achieve the purpose of Defendants' Website, are received by Defendants and stored on their server before Conversions API collects and sends the Private Information contained in those communications directly from Defendants to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

89. Although prior to discovery there is no way to confirm that Defendants have implemented Conversions API or another workaround (as that would require accessing the host server), Facebook instructs website owners like Defendants to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendants "to share website events [with Facebook] that the pixel may lose."[23]

[23] *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last access March 13, 2023).

Thus, it is reasonable to infer that Defendants are utilizing the Conversions API workaround.

90. The third parties to whom a website transmits data through pixels and associated workarounds track user data and communications for their own marketing purposes, and for the marketing purposes of the website owner. Ultimately, the purpose of collecting user data is to make money.

91. Thus, without any knowledge, authorization, or action by a user, website owners like Defendants use source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

92. In this case, Defendants employed the Pixels and Conversions API, among other tracking technologies, to intercept, duplicate, and re-direct Plaintiffs' and Class members' Private Information to Facebook and the other Pixel Information Recipients.

93. In sum, the Pixels and other tracking technologies on the Website transmitted Plaintiffs' and Class members' highly sensitive communications and Private Information to the corresponding Pixel Information Recipient, which communications contained private and confidential medical information. These transmissions were performed without Plaintiffs' or Class members' knowledge, consent, or express written authorization.

C. Defendants' Use of the Pixels Violated Their Own Privacy Policies

94. Defendants breached Plaintiffs' and Class members' right to privacy by unlawfully disclosing their Private Information to the Pixel Information Recipients. Specifically, Plaintiffs and Class members had a reasonable expectation of privacy (based on Defendants' own representations to Plaintiffs and the Class that Defendants would not disclose their Private Information to third parties.

95. Specifically, Defendants did not inform Plaintiffs that they shared their Private Information with Facebook and the other Pixel Information Recipients. Moreover, Defendants' Privacy Policy did not state that user and patient Private Information will be shared with Facebook or other unauthorized third parties. In fact, prior to a revision implemented on January 17, 2023, Defendants' Notice of Privacy Practices expressly stated "Rest Assured, Lemonaid does not sell,

rent, license, or trade your Personal Information."[24]

96. By engaging in this improper sharing of information without Plaintiffs' and Class members' consent, Defendants violated their own Privacy Policy and breached Plaintiffs' and Class members' right to privacy and unlawfully disclosed their Private Information.

97. As a "redundant" measure to ensure Plaintiffs' and Class members' Private Information was successfully transmitted to third parties like Facebook, Defendants also implemented server-based workarounds like Conversions API to send Plaintiffs' and Class members' Private Information from electronic storage on Defendants' server directly to Facebook, at a minimum.

D. Defendants' Use of the Pixels Violates HIPAA

98. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[25]

99. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

100. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

101. The Privacy Rule broadly defines "protected health information" as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

---

[24] Lemonaid Privacy Policy (April 18, 2022) https://www.lemonaidhealth.com/legals/privacy-policy (last visited June 16, 2023).

[25] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

102. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

103. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination'"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

a. Names;

…

H. Medical record numbers;

…

J. Account numbers;

…

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers; … and

P. Any other unique identifying number, characteristic, or code… and"

The covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

45 C.F.R. § 160.514.

104. The HIPAA Privacy Rule requires any "covered entity"—which includes health care

providers—to maintain appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of PHI without authorization. 45 C.F.R. §§ 160.103, 164.502.

105. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be PHI. The Department of Health and Human Services has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data, "[i]f such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI."[26]

106. Consistent with this restriction, the HHS has issued marketing guidance that provides, "With limited exceptions, the [Privacy] Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list."[27]

107. Here, Defendant provided patient information to third parties in violation of the Privacy Rule.

108. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(c), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

---

[26] *See Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, HHS.GOV (last visited June 4, 2023).

[27] *Marketing*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html, HHS.GOV (last visited June 29, 2023).

109. Defendants further failed to comply with other HIPAA safeguard regulations as follows:

a. Failing to ensure the confidentiality and integrity of electronic PHI that Defendants created, received, maintained, and transmitted in violation of 45 C.F.R. section 164.306(a)(1);

b. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);

c. Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Defendants in violation ofc45 C.F.R. section 164.308(a)(6)(ii);

d. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. section 164.306(a)(2);

e. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. section 164.306(a)(3);

f. Failing to ensure compliance with HIPAA security standard rules requiring adequate workforce comprehensive training instead of training software used to test staff by imitating phishing emails in violation of 45 C.F.R. section 164.306(a)(4);

g. Failing to effectively train its workforce (including independent contractors) on the policies and procedures for PHI as necessary and appropriate to carry out job functions while maintaining security of PHI beyond using imitation phishing email software in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and

h. Failing to design, implement, and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

110. Commenting on a June 2022 report discussing the use of Pixels by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, "I am deeply troubled by what [the hospitals] are doing

with the capture of their data and the sharing of it … It is quite likely a HIPAA violation."[28]

111. Defendants' placing a third-party tracking code on its Website is a violation of Plaintiffs' and Class members' privacy rights under federal law. While Plaintiffs do not bring a claim under HIPAA itself, this violation demonstrates Defendants' wrongdoing relevant to other claims and establishes its duty to maintain patient privacy.

E. Defendants' Use of the Pixels Violates OCR Guidance

112. In addition, the government has issued guidance warning that tracking technologies like the Pixels may come up against federal privacy law when installed on healthcare websites.

113. As mentioned previously, the HHS OCR has issued a Bulletin titled *Use of Online Tracking Technologies by HIPAA Covered Entities And Business Associates* which provides that healthcare organizations regulated under the HIPAA may use third-party tracking tools, such as Google Analytics or the Pixels *only in a limited way*, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors.[29]

114. According to the Bulletin, Defendants have violated HIPAA rules by implementing the Pixels.[30]

115. The bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI.*** Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.*** While

---

[28] '*Deeply Troubled*': *Security experts worry about Facebook trackers on hospital sites*, ADVISORY BOARD, https://www.advisory.com/daily-briefing/2022/06/17/data-trackers (last visited June 1, 2023).

[29] *See* HHS OCR Bulletin, *supra* n. 16.

[30] *See id*. ("disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures").

> it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***[31]

116. Plaintiffs and Class members face the same risks warned of above.

117. Defendants have shared Plaintiffs' and Class members' IIHI and PHI, including: search terms about health conditions for which they seek doctors; their contacts with doctors to make appointments; the names of their doctors; the frequency with which they take steps to obtain healthcare for certain conditions; and where they seek medical treatment. This information is, as described in the Bulletin, "highly sensitive."

118. The Bulletin goes on to make clear how broad the government's view of protected information is as it explains:

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, ***or any unique identifying code.***[32]

119. Crucially, the government's Bulletin continues:

> ***All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.*** This is because, ***when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.***[33]

120. Defendants' sharing of Private Information to the Pixel Information Recipients violated Plaintiffs' and Class Members' rights.

---

31 *Id.* (emphasis added.)
32 *Id.* (emphasis added.)
33 *Id.* (emphasis added.)

F. Defendants Violated Industry Standards.

121. It is a cardinal rule that a medical provider's duty of confidentiality is embedded in the physician-patient and hospital-patient relationship.

122. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

123. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)[.]

124. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

125. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must: (c) Release patient information only in keeping ethics guidelines for confidentiality.[34]

126. Defendants' use of the Pixels also violates Federal Trade Commission ("FTC") data security guidelines. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

[34] AMA Principles of Medical Ethics: I, IV, *Chapter 3: Opinions on Privacy, Confidentiality & Medical Records*, https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf, American Medical Association (last visited June 29, 2023).

127. The FTC's October 2016 publication *Protecting Personal Information: A Guide for Business*[35] established cyber-security guidelines for businesses.

128. These guidelines state that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network vulnerabilities; and implement policies to correct any security problems.

129. Defendants failed to implement these basic, industry-wide data security practices.

G. Users' Reasonable Expectation of Privacy.

130. Plaintiffs and Class members were aware of Defendants' duty of confidentiality when they sought medical services from Defendants.

131. Indeed, at all times when Plaintiffs and Class Members provided their IIHI and PHI to Defendants, they each had a reasonable expectation that the information would remain confidential and that Defendants would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

132. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

133. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[36]

134. Personal data privacy and obtaining consent to share Private Information are material to Plaintiffs and Class members.

---

[35] Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jun. 2, 2023).

[36] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/, CONSUMERREPORTS.ORG (last visited Jun. 2, 2023).

H. IP Addresses are Protected Health Information.

135. Defendants improperly disclosed Plaintiffs' and Class Members' computer IP addresses to the Pixel Information Recipients through their use of the Pixels *in addition to* unique personal identifiers such as phone numbers, email addresses, dates of birth, Defendants' client ID numbers, services selected, assessment responses, patient statuses, medical conditions, treatments, provider information, and appointment information.

136. An IP address is a number that identifies the address of a device connected to the Internet.

137. IP addresses are used to identify and route communications on the Internet.

138. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

139. Facebook tracks every IP address ever associated with a Facebook user (and with non-users through shadow profiles). Google also tracks IP addresses associated with Internet users.

140. Facebook, Google, and other third-party marketing companies track IP addresses for targeting individual homes and their occupants with advertising.

141. Under HIPAA, an IP address is considered personally identifiable information, defining personally identifiable information as including "any unique identifying number, characteristic or code" and specifically listing IP addresses among examples. 45 C.F.R. § 164.514 (2).

142. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *see also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

143. Consequently, Defendants' disclosure of Plaintiffs' and Class Members' IP addresses violated HIPAA and industry-wide privacy standards.

I. Defendants Were Enriched and Benefitted from the Use of the Pixel and other Tracking Technologies that Enabled the Unauthorized Disclosures Alleged Herein

144. The purpose of the use of the Pixels and other tracking technologies on Defendants'

Website was to improve marketing and thereby boost revenues.

145. In exchange for disclosing the Private Information of their accountholders and patients, Defendants are compensated by the Pixel Information Recipients in the form of enhanced advertising services and more cost-efficient marketing on their platform.

146. Defendants were advertising their services on Facebook, for one, and the Pixels were used to "help [Defendants] understand which types of ads and platforms are getting the most engagement[.]"[37]

147. Retargeting is a form of online marketing that targets users with ads based on previous internet communications and interactions.

148. Defendants retargeted patients and potential patients to get more people to use their services. These patients include Plaintiffs and Class members.

149. Thus, utilizing the Pixels benefits Defendants by, among other things, reducing the cost of advertising and retargeting.

150. Moreover, Plaintiffs' and Class members' Private Information had value and Defendant's disclosure and interception harmed Plaintiffs and the Class.

151. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

152. The value of health data in particular is well-known, and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[38]

153. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who

---

[37] RETARGETING, https://www.facebook.com/business/goals/retargeting, FACEBOOK. COM (last visited June 5, 2023).

[38] *See* https://time.com/4588104/medical-data-industry/ (last visited June 29, 2023).

compile the data from providers and other health-care organizations and sell it to buyers."[39]

154. Tech companies are under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own purposes, including potentially micro-targeting advertisements to people with certain health conditions.

155. Policymakers are proactively calling for a revision and potential upgrade of the HIPAA privacy rules out of concern for what might happen as tech companies continue to march into the medical sector.[40]

156. Private Information is also a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use Private Information to commit an array of crimes that include identity theft and medical and financial fraud.[41] A robust "cyber black market" exists where criminals openly post stolen IIHI and PHI on multiple underground Internet websites, commonly referred to as the dark web.

157. While credit card information and associated IIHI can sell for as little as $1–$2 on the black market, PHI can sell for as much as $363.[42]

158. PHI is particularly valuable because criminals can use it to target victims with frauds that take advantage of their medical conditions.

159. PHI can also be used to create fraudulent insurance claims, can facilitate the purchase and resale of medical equipment, and it can help criminals gain access to prescriptions for illegal use or sale.

160. Medical identity theft can result in inaccuracies in medical records, costly false claims, and life-threatening consequences. If a victim's health information is commingled with other records, it can lead to misdiagnoses or mistreatment.

---

[39] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited June 29, 2023).

[40] *Id.*

[41] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Mar. 16, 2023).

[42] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited Mar. 16, 2023).

161. The FBI Cyber Division issued a Private Industry Notification on April 8, 2014, that advised the following:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

162. Cybercriminals often trade stolen Private Information on the black market for years following a breach or disclosure. Stolen Private Information can be posted on the Internet, making it publicly available.

163. Defendants gave away Plaintiffs' and Class Members' communications and transactions on its Digital Platforms without permission.

164. The unauthorized access to Plaintiffs' and Class Members' private and Personal Information has diminished the value of that information, resulting in harm to Website Users, including Plaintiffs and Class Members.

165. Plaintiffs suffered damages in the form of (a) invasion of privacy; (b) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the invasion of privacy; (c) diminution of value of the Private Information; (d) statutory damages; (e) the continued and ongoing risk to his Private Information; (f) lost benefit of the bargain; and (g) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiffs' medical conditions and other confidential information he communicated to Defendants via the Website.

166. Plaintiffs have a continuing interest in ensuring that future communications with Defendants are protected and safeguarded from future unauthorized disclosure.

TOLLING

167. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiffs did not know—and had no way of knowing—that their Private Information was intercepted and unlawfully disclosed to the Pixel Information Recipients because Defendants kept this information secret.

CLASS ALLEGATIONS

168. This action is brought by the named Plaintiffs on their behalf and on behalf of a proposed Class of all other persons similarly situated under Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

169. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

All persons residing in the United States who used Defendants' Website.

170. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate Massachusetts Subclass, which is defined as follows:

All persons residing the state of Massachusetts who used Defendants' Website.

171. Excluded from the proposed Class are any claims for personal injury, wrongful death, or other property damage sustained by the Class; and any Judge conducting any proceeding in this action and members of their immediate families.

172. Plaintiffs reserve the right to amend the definitions of the Class or add subclasses if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

173. Numerosity. The Class is so numerous that the individual joinder of all members is impracticable. There are at least 1 million patients that have been impacted by Defendants' actions. Moreover, the exact number of those impacted is generally ascertainable by appropriate discovery and is in the exclusive control of Defendants.

174. Commonality. Common questions of law or fact arising from Defendants' conduct exist as to all members of the Class, which predominate over any questions affecting only individual Class members. These common questions include, but are not limited to, the following:

a) Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiffs and Class members;

b) Whether Defendants had duties not to disclose the Private Information of Plaintiffs and Class members to unauthorized third parties;

c) Whether Defendants violated their own privacy policy by disclosing the Private Information of Plaintiffs and Class members to the Pixel Information Recipients;

d) Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class members that their Private Information would be disclosed to third parties;

e) Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class members that their Private Information was being disclosed without their consent;

f) Whether Defendants adequately addressed and fixed the practices which permitted the unauthorized disclosure of patients' Private Information;

g) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to keep the Private Information belonging to Plaintiffs and Class members free from unauthorized disclosure;

h) Whether Defendants violated the statutes asserted as claims in this Complaint;

i) Whether Plaintiffs and Class members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

j) Whether Defendants knowingly made false representations as to their data security and/or privacy policy practices;

k) Whether Defendants knowingly omitted material representations with respect to their data security and/or privacy policy practices; and

l) Whether Plaintiffs and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendants' disclosure of their Private Information.

175. Typicality. Plaintiffs' claims are typical of those of other Class members because Plaintiffs' Private Information, like that of every other Class Member, was compromised as a result of Defendants' incorporation and use of the Pixels and/or Conversions API.

176. Adequacy. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages Plaintiffs

have suffered are typical of other Class members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

177. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class members in that all the Plaintiffs' and Class members' data was unlawfully stored and disclosed to unauthorized third parties, including the Pixel Information Recipients, in the same way. The common issues arising from Defendants' conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

178. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

179. Defendants have acted on grounds that apply generally to the Class as a whole so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

180. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a) Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information and not disclosing it to unauthorized third parties;

b) Whether Defendants breached a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c) Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d) Whether Defendants adequately and accurately informed Plaintiffs and Class members that their Private Information would be disclosed to third parties;

e) Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

f) Whether Class members are entitled to actual, consequential, and/or nominal damages and/or injunctive relief as a result of Defendants' wrongful conduct.

181. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class members' names and addresses affected by the unauthorized disclosures that have taken place. Class members have already been preliminarily identified and sent Notice by Defendants.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(*On behalf of Plaintiffs & the Nationwide Class*)

182. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

183. Upon accepting, storing, and controlling the Private Information of Plaintiffs and the Class, Defendants owed, and continue to owe, a duty to Plaintiffs and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information.

184. Defendants breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' Private Information from unauthorized disclosure.

185. It was reasonably foreseeable that Defendants' failures to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' Private Information through their use of

the Pixels, Conversions API, and other tracking technologies would result in unauthorized third parties, such as the Pixel Information Recipients, gaining access to such Private Information for no lawful purpose.

186. Defendants' duty of care to use reasonable measures to secure and safeguard Plaintiffs' and Class members' Private Information arose due to the special relationship that existed between Defendants and their patients, which is recognized by statute, regulations, and the common law.

187. In addition, Defendants had a duty under Health Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

188. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Private Information. Defendants' misconduct included the failure to (1) secure Plaintiffs' and Class members' Private Information; (2) comply with industry standard data security practices; (3) implement adequate website and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent unauthorized disclosures resulting from the use of the Pixels, Conversions API, and other tracking technologies.

189. As a direct result of Defendants' breach of their duty of confidentiality and privacy and the disclosure of Plaintiffs' and Class members' Private Information, Plaintiffs and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

190. Defendants' wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiffs' and Class members' Private Information constituted (and continue to constitute) negligence at common law.

191. Plaintiffs and the Class are entitled to recover damages in an amount to be determined at trial.

COUNT II
INVASION OF PRIVACY
(*On behalf of Plaintiffs & the Nationwide Class*)

192. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

193. The highly sensitive and personal Private Information of Plaintiffs and Class members consists of private and confidential facts and information regarding Plaintiffs' and Class members' health that were never intended to be shared beyond private communications on the Website and the consideration of health professionals.

194. Plaintiffs and Class members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this Information against disclosure to unauthorized third parties, including the Pixel Information Recipients.

195. Defendants owed a duty to Plaintiffs and Class members to keep their Private Information confidential.

196. Defendants' unauthorized disclosure of Plaintiffs' and Class members' Private Information to the Pixel Information Recipients, third-party tech and marketing giants, is highly offensive to a reasonable person.

197. Defendants' willful and intentional disclosure of Plaintiffs' and Class members' Private Information constitutes an intentional interference with Plaintiffs' and Class members' interest in solitude and/or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

198. Defendants' conduct constitutes an intentional physical or sensory intrusion on Plaintiffs' and Class members' privacy because Defendants facilitated the Pixel Information Recipients' simultaneous eavesdropping and wiretapping of confidential communications.

199. Defendants failed to protect Plaintiffs' and Class members' Private Information and acted knowingly when they installed the Pixels onto the Website because the purpose of the Pixels is to track and disseminate individual's communications on the Website for the purpose of marketing and advertising.

200. Because Defendants intentionally and willfully incorporated the Pixels into the Website and encouraged individuals to use and interact with the Website and the health services thereon, Defendants had notice and knew that their practices would cause injury to Plaintiffs and the Class.

201. As a proximate result of Defendants' acts and omissions, the private and sensitive Private Information, including the IIHI and PHI of Plaintiffs and Class members, was disclosed to unauthorized third parties, causing Plaintiffs and the Class to suffer damages.

202. Plaintiffs, on behalf of themselves and Class members, seek compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, loss of time and opportunity costs, lost benefit of the bargain, plus pre-judgment interest and costs.

203. Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information is still maintained by Defendants and still in the possession of the Pixel Information Recipients, and the wrongful disclosure of the Private Information cannot be undone.

204. Plaintiffs and Class members have no adequate remedy at law for the injuries relating to Defendants' and unauthorized third parties' continued possession of their sensitive and confidential Private Information. A judgment for monetary damages will not undo Defendants' disclosure of the Private Information to unauthorized third parties who, upon information and belief, continue to possess and utilize the Private Information.

205. Plaintiffs, on behalf of themselves and Class members, further seek injunctive relief to enjoin Defendants from intruding into the privacy and confidentiality of Plaintiffs' and Class members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT III
BREACH OF CONFIDENCE
(*On behalf of Plaintiffs & the Nationwide Class*)

206. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

207. Possessors of non-public medical information, such as Defendants, have a duty to keep such medical information completely confidential.

208. Plaintiffs and Class members had reasonable expectations of privacy in the responses and communications entrusted to Defendants through their Website, which included highly sensitive Private Information.

209. Contrary to their duties as telehealth institutions and their express promises of confidentiality, Defendants installed the Pixels and Conversions API to disclose and transmit to third parties Plaintiffs' and Class members' Private Information, including data relating to Plaintiffs' and Class members' health.

210. These disclosures were made without Plaintiffs' or Class members' knowledge, consent, or authorization.

211. The third-party recipients included, but may not be limited to, the Pixel Information Recipients.

212. As a direct and proximate cause of Defendants' unauthorized disclosures of Plaintiffs' and Class members' Private Information, Plaintiffs and Class members were damaged by Defendants' breach of confidentiality in that (a) sensitive and confidential information that Plaintiffs and Class members intended to remain private is no longer private; (b) Plaintiffs and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements; (c) Defendants eroded the essential confidential nature of health services that Plaintiffs and Class members participated in; (d) general damages for invasion of their rights in an amount to be determined by a jury at trial; (e) nominal damages for each independent violation; (f) the unauthorized use of something of value (the highly sensitive Private Information) that belonged to Plaintiffs and Class members and the obtaining of a benefit therefrom without Plaintiffs' and Class members' knowledge or informed consent and without compensation to Plaintiffs or Class members

for the unauthorized use of such data; (g) diminishment of the value of Plaintiffs' and Class members' Private Information; and (h) violation of property rights Plaintiffs and Class members have in their Private Information.

COUNT IV
UNJUST ENRICHMENT
(*On behalf of Plaintiffs & the Nationwide Class*)

213. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

214. Defendants benefit from the use of Plaintiffs' and Class members' Private Information and unjustly retained those benefits at Plaintiffs' and Class members' expense.

215. Plaintiffs and Class members conferred a benefit upon Defendants in the form of the monetizable Private Information that Defendants collected from them and disclosed to third parties, including the Pixel Information Recipients, without authorization and proper compensation.

216. Defendants consciously collected and used this information for their own gain, providing Defendants with economic, intangible, and other benefits, including substantial monetary compensation.

217. Defendants unjustly retained those benefits at the expense of Plaintiffs and Class members because Defendants' conduct damaged Plaintiffs and Class members, all without providing any commensurate compensation to Plaintiffs or Class members.

218. The benefits that Defendants derived from Plaintiffs and Class members were not offered by Plaintiffs or Class members gratuitously and, thus, rightly belongs to Plaintiffs and Class members. It would be inequitable under unjust enrichment principles in Massachusetts and every other state for Defendants to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

219. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds that Defendants received, and such other relief as the Court may deem just and proper.

COUNT V
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. § 2511(1) *et seq.*
(*On behalf of Plaintiffs & the Nationwide Class*)

220. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

221. The ECPA protects both sent and received communications.

222. The ECPA, specifically 18 U.S.C. § 2520(a), provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

223. The transmissions of Plaintiffs' and Class members' Private Information to Defendants via Defendants' Website is a "communication" under the ECPA's definition under 18 U.S.C. § 2510(12).

224. The transmission of Private Information between Plaintiffs and Class members and Defendants via their Website are "transfer[s] of signs, signals, writing, … data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

225. The ECPA defines "content" when used with respect to electronic communications to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

226. The ECPA defines "interception" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

227. The ECPA defines "electronic, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiffs' and Class members' browsers;

b. Plaintiffs' and Class members' computing devices;

c. Defendants' web-servers; and

d. The Pixels deployed by Defendants to effectuate the sending and acquisition of user and patient sensitive communications.

228. By utilizing and embedding the Pixels and Conversions API on their Website and/or servers, Defendants intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class members, in violation of 18 U.S.C. § 2511(1)(a).

229. Specifically, Defendants intercepted Plaintiffs' and Class members' electronic communications via the Pixels and Conversions API, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class members' Private Information to Facebook.

230. Defendants' intercepted communications that included, but are not limited to, communications to/from Plaintiffs and Class members regarding IIHI and PHI, including IP address, Facebook ID, and health information relevant to the screenings and treatment plans in which Plaintiffs and Class members participated.

231. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class members to the Pixel Information Recipients and, potentially, other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated 18 U.S.C. § 2511(1)(c).

232. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class members, while knowing or having reason to know that the Information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated 18 U.S.C. § 2511(1)(d).

233. Defendants intentionally intercepted the contents of Plaintiffs' and Class members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

234. Defendants intentionally used the wire or electronic communications to increase its profit margins. Defendants specifically used the Pixels and Conversions API to track and utilize Plaintiffs' and Class members' Private Information for its own financial benefit.

235. Defendants were not acting under color of law to intercept Plaintiffs' and Class members' wire or electronic communications.

236. Plaintiffs and Class members did not authorize Defendants to acquire the content of their communications for purposes of invading Plaintiffs' and Class members' privacy via the Pixels and Conversions API.

237. Any purported consent that Defendants received from Plaintiffs and Class members was not valid.

238. In sending and in acquiring the content of Plaintiffs' and Class members' communications relating to the browsing of Defendants' Website, creation of accounts, participation in Defendants' health screenings, and/or purchasing a subscription plan, Defendants' purpose was tortious and designed to violate federal and state law, including as described above, a knowing intrusion into a private place, conversation, or matter that would be highly offensive to a reasonable person.

COUNT VI
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA"), Cal. Penal Code § 631
(*On behalf of Plaintiffs & the Nationwide Class*)

239. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

240. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,

> Or
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> Or
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> Or
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

241. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

242. Each of the Pixels and Conversions API is a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

243. At all relevant times, by employing the Pixels and Conversions API, Defendants intentionally tapped, electrically or otherwise, the lines of internet communication between Plaintiffs and Class members on the one hand, and Defendants' Website on the other hand.

244. At all relevant times, Defendants aided, agreed with, employed, and conspired with the Pixel Information Recipients to use the Pixels and Conversions API to wiretap consumers to Defendants' Website and to accomplish the wrongful conduct at issue here.

245. Plaintiffs and Class members did not consent to the Pixel Information Recipients' intentional access, interception, reading, learning, recording, and collection of Plaintiffs' and Class members' electronic communications. Nor did Plaintiffs and Class members consent to Defendants aiding, agreeing with, employing, or otherwise enabling the Pixel Information Recipients' conduct.

246. The violation of section 631(a) constitutes an invasion of privacy sufficient to confer Article III standing. Unless enjoined, Defendants will continue to commit the illegal acts alleged here. Plaintiffs continue to be at risk because they frequently use the internet to search for information about products or services. They continue to desire to use the internet for that purpose, including for the purpose of acquiring healthcare services online. Plaintiffs also continue to desire to use Defendants' Website in the future but have no practical way to know if their website communications will be monitored or recorded by the Pixel Information Recipients.

247. Plaintiffs and Class members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of $5,000 per violation.

COUNT VII
VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA")
Cal. Civ. Code § 56, *et seq.*
(*On behalf of Plaintiffs & the Nationwide Class*)

248. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

249. Defendant is a "provider of healthcare," as defined in Cal. Civ. Code § 56.06, and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

250. Plaintiff and the Class are "patients," as defined in CMIA, Cal. Civ. Code § 56.05(k) ("'Patient' means any natural person, whether or not still living, who received healthcare services from a provider of healthcare and to whom medical information pertains.").

251. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals via the Pixels and Conversions API resulted from the intentional actions and negligent acts and omissions of Defendants, including

their implementation of the Pixels and Conversions API and their failure to (1) secure Plaintiffs' and Class members' Private Information; (2) comply with industry standard data security practices; (3) implement adequate website and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent unauthorized disclosures resulting from the use of the Pixels, Conversions API, and other tracking technologies.

252. Specifically, Defendant's negligence resulted in the release of Private Information pertaining to Plaintiffs and the Class to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent acts and omissions failed to preserve the confidentiality of Plaintiffs' and Class members' Private Information in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

253. Defendant's systems and protocols did not protect and preserve the integrity of electronic medical information belonging to Plaintiffs and the Class, in violation of Cal. Civ. Code § 56.101(b)(1)(A).

254. Plaintiffs and the Class were injured and have suffered damages, as described above, from Defendant's illegal disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§ 56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees, expenses and costs.

COUNT IX
VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code § 1798.80, *et seq.*,
(On behalf of Plaintiffs and the Nationwide Class)

255. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

256. Section 1798.82 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . . ."

257. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

258. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

iii. If the information is possible to determine at the time the notice is provided, then any of the following:

1. The date of the breach;

2. The estimated date of the breach; or

3. The date range within which the breach occurred.

4. As well as the date of the notice.

iv. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

vi. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

259. The disclosure of the Private Information of Plaintiffs and the Class via the Pixels and Conversions API as described herein constituted a "breach of the security system" of Defendant under section 1798.82(g) as there was "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by" Defendants. No exception applies, as the Pixel Information Recipients are neither employees nor agents of Defendants and the disclosed information was used and was subject to further unauthorized disclosure.

260. As alleged above, Defendants have not yet informed Plaintiffs and Class members about the disclosure of their Private Information although Defendant is and has been aware of such disclosure.

261. Defendant failed to disclose to Plaintiff and Class members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Private Information when Defendant knew or reasonably believed such information had been compromised.

262. Defendant's ongoing business interests gave Defendant incentive to conceal the truth about the disclosure of its users' Private Information from the public to ensure continued revenue.

263. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiff and the Class members would impede its investigation.

264. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and Class members were deprived of prompt notice of the disclosure of their Private Information and were thus prevented from taking appropriate protective measures. These measures could have prevented some of the damages suffered by Plaintiff and Class members.

265. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and Class members suffered incrementally increased damages separate and distinct from those simply caused by the disclosure of their Private Information alone.

266. Plaintiff and Class members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiff and Class members as alleged above and equitable relief.

COUNT X
VIOLATIONS OF THE MASSACHUSETTS DATA BREACH STATUTE
Mass. Gen. Laws Ch. 93h
(On behalf of Plaintiffs & the Massachusetts Subclass)

267. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

268. The acts and practices alleged herein occurred in trade or commerce in the commonwealth of Massachusetts.

269. The Data Breach, which compromised the Private Information of Plaintiffs, both Massachusetts citizens, constitutes a "breach of security," as that term is defined by Mass. Gen. Laws ch. 93H, § 3.

270. Defendants have not yet notified Plaintiffs or any other member of the Massachusetts Subclass that their Private Information was acquired and used by an unauthorized person or used for an unauthorized purpose.

271. Thus, Defendant has unreasonably delayed the disclosure of the "breach of security" of Private Information within the meaning of Mass. Gen. Laws ch. 93H, § 3.

272. Pursuant to Mass. Laws ch. 93H, Defendant's failure to timely disclose the Data Breach following discovery "as soon as practicable and without unreasonable delays" was a breach of Gen. L. ch. 93H, § 3(b).

COUNT XI
VIOLATIONS OF THE MASSACHUSETTS CONSUMER PROTECTION ACT
Mass. Gen. Law § 93a, *et seq.*
(*On behalf of Plaintiffs & the Massachusetts Subclass*)

273. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

274. Mass. Gen. Laws ch. 93A et seq. prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of Massachusetts.

275. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of G.L.c. 93A. Defendants' conduct alleged herein is a "business practice" within the meaning of G.L.c. 93A, and the deception occurred within the commonwealth of Massachusetts.

276. Plaintiffs and other members of the Massachusetts Subclass used Defendants' Website from Massachusetts. Their Private Information was collected and transmitted by operation of the Pixels, which was instantiated in the Source Code running in their browser or mobile application.

277. Defendants solicited, obtained, and stored Plaintiffs' and Class members' Private Information and knew or should have known not to disclose such Private Information to the Pixel Information Recipients through use of the Pixels and other tracking technologies.

278. Plaintiffs and Class members would not have provided their Private Information if they had been told or knew that Defendant would be disclosing such information to the Pixel Information Recipients and others.

279. As alleged herein, Defendant engaged in the unfair or deceptive acts or practices in the conduct of consumer transactions in violation of Mass. Gen. Laws ch. 93A, including but not limited to:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' Private Information from unauthorized disclosure;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information, including duties imposed by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTCA"), which prohibits "unfair . . . practices in or affecting commerce," including,

as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data, and HIPAA. Defendants' failure was a direct and proximate cause of the unauthorized disclosure of Plaintiffs' and Class members' Private Information;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class members' Private Information from unauthorized disclosure;

e. Omitting, suppressing, and concealing the material fact that it did not intend to protect Plaintiffs' and Class members' Private Information from unauthorized disclosure; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Personal Information, including duties imposed by the FTCA and HIPAA, which failure was a direct and proximate cause of the unauthorized disclosure.

280. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

281. Such acts by Defendant are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer by providing his or her Private Information to Defendant. Said deceptive acts and practices are material. The requests for and use of such Private Information in Massachusetts through deceptive means were consumer-oriented acts and thereby falls under the Massachusetts consumer protection statute.

282. In addition, Defendant's failure to secure patients' Private Information violated the FTCA and therefore violated the Massachusetts Consumer Protection Act.

283. Defendant knew or should have known that its computer systems and data security practices—in particular, their use of the Pixels and Conversions API—were inadequate to safeguard the IIHI of Plaintiffs and Class members, and that enabling third parties to collect the Private Information of Plaintiffs and the Massachusetts Subclass constituted a data breach. Plaintiffs and Class members accordingly seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

284. Defendant's violations of the Massachusetts Consumer Protection Act have an impact and general importance to the public, including the people of this commonwealth. Thousands of Massachusetts citizens have had their Private Information transmitted without consent from Defendants' Website to third parties.

285. As a direct and proximate result of these deceptive trade practices, Plaintiffs and Class members are entitled to judgment under the Massachusetts Consumer Protection Act, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

286. Defendants' implied and express representations that it would adequately safeguard Plaintiffs' and Class members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the services were of another, inferior quality), in violation of the Massachusetts Consumer Protection Act.

287. Accordingly, Plaintiffs, on behalf of themselves and Class members, bring this action under Mass. Gen. Laws ch. 93A to seek such injunctive relief necessary to enjoin further violations and recover costs of this action, including reasonable attorneys' fees and other costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, respectfully request that this Court enter an Order:

a) Certifying this case as a class action on behalf of the Nationwide Class and Massachusetts Subclass defined above, appointing Plaintiffs as representative of the Class, and appointing his counsel as Class Counsel;

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or unauthorized disclosure of Plaintiffs' and Class members' Private Information;

c) For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members;

d) For an award of damages, including but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

e) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

f) Pre- and post-judgment interest on any amounts awarded; and

g) Such other and further relief as this court may deem just and proper.

Dated: June 30, 2023

Respectfully submitted,

MIGLIACCIO & RATHOD, LLP

/s/ Matthew A. Smith

Matthew A. Smith
Nicholas A. Migliaccio*
Jason S. Rathod*
Bryan G. Faubus*
Tel: 202.470.3520
msmith@classlawdc.com
nmigliaccio@classlawdc.com
jrathod@classlawdc.com
bfaubus@classlawdc.com

**pro hac anticipated*

Attorneys for Plaintiffs & the Putative Class